DETEKSI FAST FLUX PADA *PASSIVE DNS*

BERBASIS METODE *SUPPORT VECTOR MACHINE* (SVM)

TUGAS AKHIR

Diajukan Untuk Memenuhi

Persyaratan Guna Meraih Gelar Sarjana

Informatika Universitas Muhammadiyah Malang

Risdalita Mauliya

201610370312230

Jaringan

PROGRAM STUDI INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS MUHAMMADIYAH MALANG

2018

LEMBAR PENGESAHAN

Deteksi *Fast Flux* pada *Passive DNS* Berbasis Metode *Support Vector Machine (SVM)*

Tugas Akhir

Telah diesahkan Guna Meraih Gelar Sarjana Strata 1
Teknik Informatika Universitas Muhammadiyah Malang

Disusun Oleh:
Risdalita Mauliya
201610370312230

Tugas Akhir ini telah diuji dan dinyatakan lulus melalui sidang majelis penguji pada tanggal 26 Oktober 2018

Menyetujui,

Dosen Penguji 1	Dosen Penguji 2
Evi Dwi Wahyuni, S.Kom, M.Kom.	**Didih Rizki, S.Kom, M.Kom**
NIDN. 0718108701	**NIDN. 0702109201**

Mengetahui,
Ketua Jurursan Teknik Informatika

Cita Indah, M.ST.,M.Kom.
NIDN. 0720038101

KATA PENGANTAR

Segala puji syukur kepada Allah SWT Maha Pengasih lagi Penyayang, atas berkat Rahmat dan Ridho-Nya beserta shalawat dan pujian kepada Nabi Muhammad SAW, penulis selama ini dapat menyelesaikan tugas akhir ini, sehingga pada akhirnya penulis dapat menyelesaikan tugas akhir yang berjudul **"DETEKSI *FAST FLUX* PADA *PASSIVE DNS* BERBASIS METODE *SUPPORT VECTOR MACHINE (SVM)*"** dapat diselesaikan dengan baik.

Pada kesempatan ini penulis menyampaikan rasa terima kasih yang sebesar-besarnya kepada orang-orang yang telah berperan sehingga dapat terselesaikannya tugas akhir ini, antara lain :

1. Untuk Ayah dan Ibu tercinta serta semua keluarga tercinta dirumah (Ka Resti, Ka Ridha) yang selalu mendoakan, memberikan nasihat, memberikan dukungan moril maupun materil selama menempuh pendidikan di Universitas Muhammadiyah Malang. Aku menyayangi kalian.
2. Dr. Fauzan, M.Pd selaku Rektor Universitas Muhammadiyah Malang.
3. Gita Indah, M.ST., M.Kom selaku Ketua Jurusan Teknik Informatika Universitas Muhammadiyah Malang.
4. Eko Budi Cahyono, S.Kom., M.T. selaku dosen pembimbing utama yang telah meluangkan banyak waktu, tenaga, dan pikiran dalam memberikan pengarahan dalam penulisan tugas akhir ini.
5. Yufis Azhar, S.Kom., M.Kom selaku dosen pembimbing pendamping yang telah meluangkan banyak waktu, tenaga, dan pikiran dalam memberikan pengarahan dalam penulisan tugas akhir ini.
6. Teruntuk partner terbaik Vinna Utami Putri, teman seperjuangan kuliah sampai tugas akhir, wisuda bareng-bareng hingga kuliah lagi disini dan terjadi lagi. Semoga selalu diberikan keselamatan dan kebahagiaan untukmu.
7. Teruntuk sahabatku, Vinna Utami Putri, Izmi Izwati Adistia, Novinta Nurmasari, Ghina Arih Juliani, Auni Aulia Muftiany, Giffary Esa T., Rifqi Khairanoor, dan M. Yusuf Anwar yang telah membantu dorongan, semangat, keceriaan yang didapatkan. Moments disini akan selalu terkenang seumur hidup. Aku menyayangi kalian.

8. Teman – teman dikampus yang telah membantu dalam memberikan arahan dan bimbingan dalam pengerjaan tugas akhir ini tanpa kalian aku tidak bisa apa-apa.
9. Pihak-pihak lain yang telah memberikan bantuan secara langsung maupun tidak langsung dalam pembuatan tugas akhir ini yang tidak dapat disebutkan satu persatu.

Penulis menyadari bahwa penulisan skripsi ini masih jauh dari sempurna. Oleh karena itu, penulis mengharapkan segala petunjuk, kritik, dan saran yang membangun dari pembaca agar dapat menunjang pengembangan dan perbaikan penulisan selanjutnya.

Akhir kata penulis mohon maaf atas kekurangan dalam penulisan tugas akhir ini dan penulis dengan senang hati menerima saran dan kritik yang membangun dari pembaca.

Semoga tugas akhir ini dapat berguna untuk menambah wawasan dan wacana bagi rekan-rekan mahasiswa.

Malang, Oktober 2018

Penulis

DAFTAR ISI

UNIVERSITAS MUHAMMADIYAH
MALANG

DAFTAR GAMBAR

DAFTAR TABEL

Daftar Pustaka

[1] D. Ardiantoro, “P e n g a n t a r D N S (D o m a i n N a m e S y s t e m),” pp. 1–4, 2003.

[2] P. Marques and H. V. Ru, “Botnet Detection Using Passive DNS,” 2014.

[3] J. Jimiwal, “Fast Flux &Fast Flux Detection Techniques:ASurvey,” vol. 3, no. 5, pp. 1708–1713, 2014.

[4] L. Bilge, E. Kirda, C. Kruegel, M. Balduzzi, and S. Antipolis, “EXPOSURE : Finding Malicious Domains Using Passive DNS Analysis.”

[5] J. Nazario and T. Holz, “As the Net Churns : Fast-Flux Botnet Observations Tracking Fast-Flux Domains,” 2008.

[6] P. Porras, H. Sa, P. Porras, and H. Sa, “A Multi-perspective Analysis of the Storm (Peacomm) Worm A Multi-perspective Analysis of the Storm (Peacomm) Worm,” no. 650, 2007.

[7] T. Moore and R. Clayton, “An Empirical Analysis of the Current State of Phishing Attack and Defence,” pp. 1–20.

[8] C. Hsu, C. Huang, and K. Chen, “Fast-Flux Bot Detection in Real Time.”

[9] A. Caglayan, M. Toothaker, D. Drapaeau, D. Burke, and G. Eaton, “Behavioral Analysis of Fast Flux Service Networks,” 2009.

[10] R. Perdisci, I. Corona, D. Dagon, and W. Lee, “Detecting Malicious Flux Service Networks through Passive Analysis of Recursive DNS Traces Detecting Malicious Flux Service Networks through Passive Analysis of Recursive DNS Traces,” no. December 2009, 2015.

[11] E. Stalmans and B. Irwin, “Geo-Spatial Autocorrelation as a Metric for the Detection of Fast-Flux Botnet Domains,” no. January 2016, 2012.

[12] X. Y. B. Z. L. K. and J. Chen, “FF deteksi svm.pdf.” Information Technology Journal 11, China, 2012.

[13] M. Yunus, “Penerapan Konsep Data Mining Pada Database Akademik STMIK Pradnya Paramita Dengan Delphi,” pp. 35–46.

[14] U. Fayyad, “The KDD Process for Extracting Useful Knowledge from Volumes of Data,” vol. 39, no. 11, pp. 27–34, 1996.

[15] D. Mining, K. Discovery, and I. N. Databases, “Konsep Data Mining,” 2009.

[16] U. P. JAYA, “Konsep Data Mining.”

[17] H. Sahu, S. Shrma, and S. Gondhalakar, “A Brief Overview on Data Mining Survey,” vol. 1, no. 3, pp. 114–121, 2008.

[18] I. U. Nadhori and F. T. Industi, “Pendeteksian Trafik Anomali pada Jaringan didasarkan pada Analisa Payload Data Berbasis Metode Support Vector Machines,” pp. 98–102, 2009.

[19] A. S. Nugroho, A. B. Witarto, and D. Handoko, “Support Vector Machine,” 2003.

[20] R. Munawarah, O. Soesanto, and M. R. Faisal, “PENERAPAN METODE SUPPORT VECTOR MACHINE,” vol. 04, no. 01, pp. 103–113, 2016.

[21] P. da Pedro Marques Luz, “Botnet Detection Using Passive DNS,” *Thesis Ru.Nl*, p. 41, 2014.

[22] M. D. Data and S. Features, “Mining DNS-related Data for Suspicious Features Tilman Frosch,” 2011.

[23] E. Soltanaghaei and M. Kharrazi, “Detection of fast- ux botnets through DNS tra c analysis,” no. January 2016, 2018.